Introduction

The outcome of the relationship between risk professionals and line managers should be value-added in terms of both tangible contributions to performance-oriented decisions and perceived benefits resulting from insights not otherwise considered. In these dynamic times, effective organizations constantly challenge themselves on worst-case scenarios; they are, and should be, their own devil’s advocate.

In a white paper issued in late 2010, The Name of the Game is Risk: Secrets of the Winning Hand, we inaugurated a series addressing the critical challenges being faced by today’s financial services chief risk officers (CROs). We used the game of poker as an analogy to define five secrets of what we referred to as the “winning hand” for CROs. While there continue to be developments and much discussion in the financial services industry regarding enhanced oversight, more rules and regulations, increased transparency, and better governance, among other issues, the question arises as to whether such changes will make a significant difference going forward. If the secrets we cited in the aforementioned white paper are not addressed, we believe chances are the changes being implemented across the industry will fall short of expectations.

One of the five secrets was constructive board engagement, and the second issue of our CRO Series focused on the current state of board risk oversight, leveraging data from Protiviti’s Board Risk Oversight survey sponsored by COSO. This secret is about enabling the CRO’s success through effective board risk oversight.

This third installment of our CRO Series addresses another secret, effective positioning of the risk management organization. The CRO is responsible for executing the risk program and providing another line of defense in protecting enterprise value. No other individual, function or group in a financial institution is charged with viewing performance exclusively from a risk perspective – not internal audit, not legal, not executive or line management. The secret is not simply to have a risk management organizational structure with names in boxes on a chart, but rather to have knowledgeable professionals take an objective, often contrarian, perspective about a strategy, plan, transaction or deal without repercussions to their compensation and careers – a perspective that is appreciated and expected by executive and line management. The CRO’s purpose is not to get along, but to protect enterprise value that may have taken decades for the institution

---


to build. Simply stated, the question is whether risk management is positioned to be successful within the organization. CROs with successful programs achieve a high level of collaboration between business and risk teams that is founded on mutual respect for what each brings to the conversation. In essence, they have a seat at the table.

**Key Success Factors for Positioning**

While risk management function positioning is not a one-size-fits-all solution, there are fundamental principles that make it work. The outcome of the relationship between risk professionals and line managers should be value-added in terms of both tangible contributions to performance-oriented decisions and perceived benefits resulting from insights not otherwise considered. In these dynamic times, effective organizations constantly challenge themselves on worst-case scenarios; they are, and should be, their own devil’s advocate. Such a cynical view forces critical thinking and shifts energy to optimal performance in a risky environment over time.

When risk professionals are excluded from key decision points, when their views are dismissed with little regard, or when they are placed in a role that is merely consultative and collaborative with no meaningful authority, then line management does not have the organization’s best interests in mind, or the risk professional is a poor communicator of his or her value, or the risk professional is unable to overcome his or her weak positioning within the organization, or all of the above. In any of these cases, the organization is placed in a precarious position of overreliance on people who may be thinking more about their own self-interest than the long-term interests and viability of the organization. If the board is not sufficiently engaged, then the organization lacks the benefit of a true risk perspective. If powerful business line managers dismiss risk professionals as a “check-the-box” obligation, a fatal flaw in risk management emerges. If the chief executive officer (CEO) is constantly arbitrating front- and back-office disagreements on significant risk issues without knowledge of the board, directors lack vital insights into the institution’s risk culture.

At the crucial moment when someone must play a contrarian role to protect the shareholders’ interests, how can a CRO ever stand down a CEO who is driven to achieve performance goals at any cost when that CEO controls the CRO’s career progression, salary and bonus? And if the CEO doesn’t believe in the value of risk management, it’s game over, as risk doesn’t have a meaningful voice at the table when it is really needed.

The secret of risk management team positioning is to establish an organizational structure that enables dissention and cooperation and leads to a risk culture desired by the board. In the sidebar on the next page, we summarize the elements of ineffective positioning. If we were to turn these red flags around, we can construct six key success factors for risk management positioning:

1. The CRO is viewed as a peer with business line leaders in virtually all respects (e.g., compensation, authority and direct reporting to the CEO) and likewise down through the business hierarchy and across the organization.

2. The CRO has a dotted reporting line to the board or a committee of the board and faces no constraints of any kind in reporting to the board.
3. The board, senior management and operating personnel believe that managing risk is an organizational imperative and everyone’s job.

4. Management values risk management as an equal discipline to opportunity pursuit.

5. The CRO is clearly viewed as undertaking a broader risk focus than compliance.

6. The CRO’s position and how it interfaces with senior line and functional management is clearly defined.

While these attributes may not be all-inclusive, they represent key success factors that result in a significant step forward to ensuring the risk management function process is impactful, which sets the tone for an effectively functioning CRO.

**Elements of Ineffective Positioning**

The following are signs of ineffective positioning of the CRO within the organization:

- The CRO is not viewed as a peer with business line leaders in virtually all respects (e.g., compensation, authority and direct reporting to the CEO).

- The CRO has no reporting line to the board or faces formidable constraints in reporting to the board that he/she cannot be reasonably expected to overcome when escalation of risk issues to the board is necessary.

- The board, senior management and operating personnel believe that managing risk is a single person’s or function’s job and is not an organizational imperative or everyone’s job.

- Management does not value risk management as a discipline equal in importance to opportunity pursuit, or sees it as a necessary compliance function, or worse – as a blocker to getting things done.

- The organization views the CRO function as primarily a compliance management activity.

- There is lack of clarity/definition in the CRO position and how it interfaces with senior line and functional management, leaving the CRO constantly justifying his/her place in the conversation or fighting turf issues.

One or more of these elements may signify a red flag that the CRO (or an equivalent executive) is unable to fulfill the strategic demands of the job and lacks real authority or influence. As a result, risk management may be set up to fail.
The Current State of Positioning

The CRO function continues to increase in stature with more CROs reporting to the CEO and/or to the board of directors and becoming more engaged with the lines of business in their business strategy-setting and planning activities. In general, the prevailing view is that the risk organization cannot simply be a compliance function and/or a reporting and measurement function.

In January 2010, Protiviti conducted a review of the CRO function at 15 financial institutions to obtain an understanding of their organizational structure. We subsequently updated our review in 2012. In the 2010 review, we found that the CRO function had experienced significant change in response to the financial crisis. At that time, banks were generally focused on improving the scope, size and organizational design of the CRO function. While there was no one-size-fits-all approach and multiple models existed among the various institutions, three notable observations surfaced in our 2010 review:

- A significant majority of the CROs reported to the CEO, with some CROs also reporting to a committee of the board of directors. The formality of reporting relationships and a trend indicating more boards were conducting periodic executive sessions with the CRO provided clear evidence that CROs were getting increased visibility both within the organization and with the board, providing them the opportunity to escalate risk issues on a timely basis.

- At the time of the review, there were external regulatory and “best practice” pressures to create solid-line reporting relationships to the CRO for embedded “line of business” or “product” level risk officers so that the reach and independence of the risk management organization could be extended across the institution. Depending on the reporting relationship of embedded risk functions, full-time equivalent (FTE) leverage models continued to vary widely, ranging from more than $10 billion of assets per FTE to $125 million per FTE.

- The CRO’s functional responsibility existed across the vast majority of the organizations in such areas as credit risk, market risk, compliance and operational risk. Model validation was an emerging area of responsibility for CROs in many institutions. Some CROs were chairing or participating in management risk committees. In addition, development and improvement of the bank’s risk appetite framework was viewed as a key initiative undertaken by several CROs.

During our 2012 review, we found that the CRO function continued to increase in stature, with more CROs reporting to the CEO and/or to the board of directors and becoming more engaged with the lines of business in their business strategy-setting and planning activities. In general, the review noted a prevailing view that the risk organization cannot simply be a compliance function and/or a reporting and measurement function. To be effective, the risk organization must contribute the insights and comprehensive analysis needed to ensure appropriate balance in key management decisions. This point of view makes a lot of sense.
in light of lessons learned from the financial crisis (i.e., there must be a more balanced focus on protecting institutional value, as well as on creating it). Our 2012 review noted that risk organizations continued to expand with the objective of providing appropriate centralized oversight and guidance to ensure consistent, comprehensive risk management practices, with such expansion respecting the desire for business units to retain accountability for risk.

In March 2011, the Economist Intelligence Unit published a study with global reach that provided insight as to the current state of risk positioning in financial services institutions, particularly with regard to risk culture. According to the study, only one-half of the participating institutions reported that their risk functions had gained authority over the previous 12 months, leaving a significant percentage of institutions reporting that the authority of their risk functions had either remained the same or declined. Most importantly, almost one in four institutions reported that the views of their risk functions were more often than not overridden or ignored in their organization. Also, the study noted that while the role of the risk function had elevated since the financial crisis, risk managers at many institutions were having a difficult time building strong and open relationships with other parts of the business. One contributing factor was poor communication between departments. This silo mentality served as a barrier to effective risk management, particularly with the business units.3

Each of our reviews in 2010 and 2012 also indicated that risk culture continues to be a work in progress. To that end, improvement is still needed in at least two areas. First, while there has been progress in becoming more engaged with the lines of business, more work is needed to cement these ties and make them work effectively. Second, more progress is needed in embedding risk management considerations into performance evaluations and compensation structures. Both of these goals are likely to take some time to accomplish.

The above results indicate that since the financial crisis, the bar has been raised on risk management. While that’s a good thing, to shift the organizational culture to instill a mindset of awareness and ownership of risk, management must commit significant time and effort to establish policies, monitor progress and make substantial investments in processes and systems to support fundamental change. Changing deeply ingrained attitudes toward risk requires significant attention to managing how people focus on risk.

From a regulatory standpoint, the view is that the area of risk governance may have experienced the most significant amount of change in the financial services industry since the financial crisis. This improvement was confirmed by the Senior Supervisors Group (SSG) in their 2009 report:

Organizational changes have focused on strengthening the chief risk officer position, with the introduction of more independent reporting lines, greater stature and authority on management and other committees, and, at a number of firms, direct involvement in business line compensation decisions. At most firms, risk management personnel assigned to business lines now formally report to the firm’s chief risk officer and, in many cases, retain a weaker, “dotted-line” reporting responsibility with the business line executive. A few outlier firms, however, have yet to sever the joint reporting lines of risk management personnel to both the business line and the independent risk management function.4

In summary, the good news is that CROs are making progress in gaining a seat at the decision-making table. That said, additional improvements are possible at many organizations to further enhance the effectiveness of both the top-down risk oversight and bottom-up line involvement in managing key risks across the enterprise, especially with respect to risk culture.

4 Risk Management Lessons from the Global Banking Crisis of 2008, October 2009, issued by the SSG, page 23. The SSG is comprised of senior executives from the bank supervisory authorities of the United States, Canada, France, Germany, Japan, Switzerland, the United Kingdom and other countries. The SSG asked 20 major global financial institutions in their respective regulatory jurisdictions to assess their risk management processes to ascertain whether there were any gaps with previously issued industry or supervisory recommendations. The surveyed financial institutions completed these self-assessments during the first quarter of 2009, presented the results to both their boards of directors and their primary supervisors, and then submitted the results to the respective SSG member. The various submissions were used by the SSG to compile its report.
Steps Companies Can Take to Improve CRO Positioning

While some may argue it is important for the CRO to be a “team player,” that argument misses completely the vital point that the CRO must occasionally offer a contrarian voice as well as alternative views of the future; otherwise, the decision-making process is flawed with “group think.”

While some may assert that the ultimate advocate for risk management in the enterprise is the CEO, the CRO role is unique in that the person placed in this role is expected to provide the voice that champions the protection of enterprise value at the crucial decision-making moment when a contemplated strategy, transaction or deal is likely to expose the organization to unacceptable risk. While some may argue it is important for the CRO to be a “team player,” that argument misses completely the vital point that the CRO must occasionally offer a contrarian voice as well as alternative views of the future; otherwise, the decision-making process is flawed with “group think.” The CRO is concerned with considering what the institution may not know and evaluating the “big picture” view of enterprise risk, risk profiles and risk alignment. The crux of the positioning question we explore in this paper is, “Does anyone care?”

As one of the aforementioned studies noted, almost nine of 10 executives interviewed indicated that the CRO function has been strengthened since the financial crisis, with more than a third reporting a significant increase. While this is good news, only 23 percent reported a significant shift in institutionalizing comprehensive, consistent and collaborative approaches to risk. Therefore, there are opportunities for improving CRO positioning.

We offer several considerations below, using our six key success factors for CROs as a discussion framework:

1. Viewed As a Peer With Business Line Leaders

Every institution should ask the following question: “Do we devote enough attention to thinking about what we don’t know?” An indicator of the quality of the assessment process is the extent to which the risks considered represent a potential event or combination of events that we currently know to be possible, but do not know whether they will materialize. The more “unknowns” an organization is able to identify and evaluate in the risk assessment process, the more effective the process will be and the more anticipatory and better prepared the company will be as it faces the future. In short, business line leaders need the forward-looking risk perspective the CRO is expected to provide. For this collaborative relationship to work, they must view the CRO as a peer.
The only way they will do that is if the CRO is rewarded with equivalent compensation and has the scope of responsibilities, authority and direct reporting lines that demand respect. The total package of actively participating in the strategy-setting process, leading the formulation of the organization’s risk appetite statement, developing risk reporting mechanisms, chairing/participating in management risk committees and, when appropriate, escalating risk issues to the CEO and the board must convey to the lines of business and across the institution that the CRO is a player.

**Implication:** If the CRO is not viewed as a peer with business line leaders, the CEO and board need to consider what they intend to accomplish with the risk management function and evaluate whether to make the necessary adjustments to strengthen how it is positioned. We believe that positioning the CRO as a direct report to the CEO is critical to sending the right message.

2. **Board Reporting and Interactions**

Consistent with the premise that risks must be owned by the lines of business that generate them, the CRO does not typically own responsibility for managing specific risks, but generally operates in a strategic oversight role with authority vested by the executive committee (or a designated risk management committee), the CEO and/or the board (or a committee of the board). It is this strategic oversight focus that begs the question of how the CRO should be positioned to maximize his or her effectiveness. We believe that direct reporting to the CEO with open and free access to the board (or a board subcommittee) is sound practice. In any reporting structure, we believe there are five important principles to consider.

- The CRO should report directly to the CEO, as noted earlier.
- There should be dotted-line reporting to the board or a committee of the board (e.g., the CRO reports to the risk committee of the board on a dotted-line basis while chairing the executive risk committee).
- The CRO must not face any constraints in reporting to the board.
- Boards should conduct periodic executive sessions with the CRO – these sessions should be mandatory and regularly scheduled.
- A formalized escalation process should exist (e.g., written procedures and agreements requiring escalation of any significant issues raised by the risk management function that are being argued by line-of-business executives).

For the above principles to work effectively in practice, the board and CEO must have mutual understanding of the CRO’s role and function with the intent of preserving the CRO’s independent role within the organization.

**Implication:** The board must be vigilant to ensure there is nothing constraining the CRO from reporting to it when risk issues arise. Periodic executive sessions with the CRO can help in this regard. As for a formalized escalation process, even in circumstances where the CEO resolves disputes between the first and second lines of defense, the board should be informed to the extent such disputes are about significant or material matters. In addition, the CRO’s compensation and career must be insulated if the hopefully rare circumstance arises when he or she differs with the CEO.
There must be an explicit acknowledgement that prudent limits to entrepreneurial value-creating activities are an important aspect to governing the execution of the institution’s business model. ... If this objective is not a shared value in the organization, then executive management and the board need to take a step back and clarify what they really want the risk management function to accomplish.

3. Managing Risk Is Everyone’s Job

Neither of the two points above or the three points below matter if the board, senior management and operating personnel believe that the CRO is the only person within the organization who is concerned with risk. Unless managing risk is an organizational imperative, with line personnel aware of and owning the risks their operations create, it is really difficult for any CRO to be successful.

Implication: This point is much more than a policy matter. It is a risk cultural issue warranting close attention by the CEO and the board and the maintenance of appropriate policies, processes and systems that institutionalize a comprehensive, collaborative approach to managing risk. It takes time for such a culture to evolve.

4. Risk Is Equal to Opportunity Pursuit

Given the complexity of the business environment, the board needs to know that management is being careful to avoid the overconfidence that is bred by a single or “official” view of the future. Overconfidence is a powerful source of illusions, and is often driven by the degree of success senior and line managers have experienced and the quality and coherence of the storyline they construct regarding the future they envision to rationalize the actions they take in the present. “What if” scenario planning and stress testing are tools for evaluating management’s “view of the future” by visualizing different future conditions or events, what their consequences or effects might be on the institution’s revenues, costs, profits and market share, and how the organization might respond to or benefit from those conditions or events. For these tools to be effective, and for the CRO to be successful in using them to impact the decision-making process, there must be an explicit acknowledgement that prudent limits to entrepreneurial value-creating activities are an important aspect to governing the execution of the institution’s business model. Everyone who matters in the organization must share the view that it is in the best long-term interests of the institution to strike an appropriate balance between (a) enterprise value creation activities and (b) control mechanisms intended to protect enterprise value, so that neither one is too disproportionately strong relative to the other. If this objective is not a shared value in the organization, then executive management and the board need to take a step back and clarify what they really want the risk management function to accomplish.

Implication: There will always be tension within an institution between market-making and control activities. However, striking the appropriate balance between the two is fundamental to what a CRO attempts to achieve and typically begins with formulating and documenting a risk appetite statement. From there, risk management considerations are incorporated into performance evaluations, compensation decisions and the discipline of monitoring the impact of changes in the business environment on the institution’s risk profile over time. These activities should improve and shape the risk culture of the institution.
5. Broaden Focus Beyond Compliance

The CRO’s focus must be on understanding enterprise risk, monitoring changes in the risk profile and aligning risk with the desired tolerances for risk. This is a tough job. Compliance risks are an important subset of the enterprise’s overall risk profile, along with strategic, operational and financial risks. Focused on compliance with laws, regulations and internal policies, compliance risk management is also a very demanding task in a financial institution. Therefore, the CRO should be careful not to focus on compliance matters to the detriment of considering other risks. While in many institutions the chief compliance officer reports to the CRO function, the CRO does not want the organization to perceive his or her role as primarily a compliance function that forces the business to follow rules imposed on it. If risk management is perceived as a check-the-box compliance activity, the CRO will have difficulty achieving peer status with business line leaders and will likely not have the desired impact at the crucial moment when a contrarian voice is needed. All that being said, compliance risks are an integral component of the institution’s risk profile, and the CRO should ensure that such risks are being managed effectively.

Implication: While it is important to the CRO that the organization is in full compliance with applicable laws, regulations and internal policies, he or she should also provide appropriate focus on strategic, operational and financial risks. In the current environment, compliance is likely one of the top three risk areas for most financial services organizations and even the No. 1 risk for many institutions. Therefore, the CRO may have to devote more attention to compliance than he or she otherwise would during times with less active regulatory activity. The CRO’s challenge is to keep his or her focus on compliance at a strategic level, which is good advice for all risk types, whether the topic is compliance, fraud, vendor management, technology or any other type of risk.

6. Clearly Defined CRO Position

A CRO should be positioned within the organization to enhance his or her objectivity, both in fact and in appearance. If hired from within, the CRO must be careful not to lose focus on the broader enterprise view of risk by placing undue focus on the “comfort zone” of his/her former functional area or line of business. Ideally, the CRO is accountable for enabling the efficient and effective governance of all truly significant risks, and the related opportunities, for the institution overall and its various segments. To play this role effectively, the CRO needs to adopt an enterprisewide perspective, have a thick skin, exercise healthy skepticism, question everything he or she does not understand and be forward-looking. Furthermore, the CRO should not have a need for lasting workplace friendships.

As with any CEO direct report, the CRO should be accountable to the CEO, executive management and the board for enabling the institution to balance risk and reward and preserve enterprise value and reputation. For example, he or she should:

- Establish and communicate the organization’s risk management vision
- Design and implement an appropriate risk management infrastructure
- Establish, communicate and facilitate the use of appropriate risk management methodologies, tools and techniques
- Facilitate enterprise risk assessments and monitor the capabilities around managing the priority risks across the institution
- Implement appropriate/meaningful action-oriented risk reporting to the overall board, specific board committees and senior management
• Determine the appropriate mix of centralized and decentralized approaches to establishing risk policy and standards, defining risk appetite, and setting risk thresholds and limits

• Review compensation plans to consider the impact of risk factors and the compensation structure on behavior

To be truly objective and effectively positioned within the organization so as to enhance the appearance of objectivity, the CRO should be insulated from and independent of business unit operations. In addition, if one or more risk units reports to the CRO (such as compliance), it is important that the CRO does not overly focus on the management of certain risks to the detriment of (a) undertaking an enterprise approach to understanding the risk profiles of the institution as a whole and of specific lines of business and (b) evaluating the impact of change on those risk profiles.

Implication: The key here is to understand what the CEO and board want. Do they want an objective assessment of the risks resulting from a line of business, transaction, deal or business plan, broken down into the fundamental components of risk so they can be measured and systematically evaluated and managed? If a strategy, plan, transaction or deal is inconsistent with the desired risk profile, do they want to know what action can be taken to align it accordingly? At the other extreme, do they want someone to exercise veto power with a narrow view of complying with regulatory requirements? Based on the expectations of the CEO and the board, the CRO’s role must be defined accordingly. Ideally, CROs should improve proposed business plans, transactions and deals so that they are more likely to succeed in creating enterprise value, while also taking prudent steps to protect enterprise value.

These are steps companies can take to improve risk culture and position their CRO to assist management with providing sufficient attention to risk management and to offer the board a strong and respected independent view on critical risks and risk management issues.
How the CRO Can Improve Positioning

The depth and breadth of the CRO’s relationships with senior executives and business line leaders have a significant impact on his or her effectiveness and the sustainability of the position as it is defined.

It should be apparent in the above discussion that the CRO can and should be an effective facilitator and enabler with respect to all six key success factors for positioning risk management and the CRO function. In addition, the other four secrets underlying a successful CRO come into play here. For example:

- Effective board risk oversight forces discussion of critical issues that can strengthen the CRO’s positioning within the organization.
- Both the board and the CRO can drive integrity to the discipline of risk management.
- The CRO plays a vital role in establishing a learning culture for risk management across the organization.
- The CRO can be an integral part of the institution’s process for ensuring incentives set for value-creating pursuits encourage the desired behaviors.

In terms of the role the CRO can play in improving positioning, it may help first to determine the baseline organizational structure by defining what is currently being done. The sidebar beginning on the next page provides illustrative questions to consider in this regard.

The resulting “current state” assessment of the risk governance organizational structure should be evaluated to identify enhancements and improvements that could strengthen the CRO’s contribution. Recommendations can be developed through comparison of the institution’s organizational structure and practices against other institutions through networking with other CROs and drawing insights from benchmarking surveys. Most importantly, regulatory guidance and directives should be considered to understand the expectations of the supervising agencies. The results of this analysis should be reviewed with the CEO and the board and the resulting gaps addressed.

Since we are not talking about a one-size-fits-all approach, there are no “hard and fast” rules here. The key is the end objective. What do the CEO and board want and what do regulators expect? Conversely, what opportunity for value contributed does the CRO see? The board’s agenda, the CEO’s strategic focus, management’s operating style, the nature of the institution’s risks, the effectiveness of its capabilities for managing those risks, the gaps in managing the institution’s risks, and the cost and cultural implications of the CRO’s activities are all factors in determining the CRO’s role and positioning.

1 These four additional secrets are discussed in *The Name of the Game Is Risk: Secrets of the Winning Hand*, as noted in Footnote 1. They are (1) integrity to the discipline of risk management, (2) effective board risk oversight, (3) establishing a learning culture for risk management across the organization, and (4) ensuring appropriate incentives for value-creating pursuits.
The more risk management is seen as a source of competitive advantage over the long term, and the greater
the perceived need for forward-looking indicators of risk and increased investment in risk management
infrastructure, the more likely the CRO will have a seat at the table, setting strategy and risk appetite,
participating in product development and formulating M&A strategy, and evaluating compensation structures.
On the other hand, the CRO’s role is likely to be more limited if: his or her accountability is limited to certain
specific risk areas (e.g., credit, compliance, etc.); the interface with strategy-setting is to assess suitability after
the fact; the focus is no more than regulatory compliance and consistent shareholder returns; the line of sight
is on a reactive approach to risk management policy; risk management investments are constantly deferred;
risk management is fragmented and siloed; and enterprise risk management is merely viewed by management
as “the sum of the parts.”

Positioning of the CRO function within the organization is more than defining the role. The depth and
breadth of the CRO’s relationships with senior executives and business line leaders have a significant impact on
his or her effectiveness and the sustainability of the position as it is defined. The stronger those relationships
(in terms of mutual respect and recognition of value contributed), the more effective the CRO will be in
realizing the intended value proposition. As with everything else and everyone else, delivery on expectations is
huge. As expectations increase, the need for more sophisticated risk professionals grows.

Some Questions to Consider When Evaluating a “Current State” Risk Governance Structure

While there is no one-size-fits-all approach, there are several design principles relating to the risk
governance roles and authorities at various levels of the organization, as expressed by the questions
below:

• What are the roles of the board and the CEO in providing risk oversight? Effective risk
management starts at the top.

• Does the management executive committee allocate sufficient time to focus on risk management
issues?

• Is there a separate executive risk committee? If so:
  – What is its composition?
  – What are its roles and responsibilities?
  – How does it interface with the strategy-setting process?
  – How does it interface with the operating and functional units, as well as with the board?
  – Does it have a charter?
  – What risks does it oversee and govern?

• Does the organization designate a single officer to assume certain overall responsibilities for risk
management (e.g., a CRO or equivalent executive)? If yes:
  – Is he/she independent of the core business activities?
  – To whom does he/she report (e.g., to the CEO, another C-level executive and/or to the board of
directors or a standing committee of the board)?
  – What are his/her overall role and responsibilities, as articulated in the job description?
  – Is his/her role authoritarian (approve and escalate)? If not, what is it, e.g., consultative (assess,
advise, recommend, champion)?
  – Is he/she responsible for developing and/or coordinating execution of the overall risk
management framework?
– Does he/she chair the institution’s executive risk committee?
– Does he/she serve as a designated liaison with regulators?
– Is there adequate support staff to enable the executive to carry out his or her responsibilities?

• What are the roles and responsibilities of lines of business and functional units (e.g., IT, legal, HR, etc.) as they relate to managing risk?

• What governance or independent validation units are there (e.g., internal audit, model risk/validation, compliance management, value-at-risk review and other risk management back-office activities)? To whom do they report, and how often?

• To what extent should management of risks be centralized (i.e., all personnel with risk management responsibilities report through the CRO’s line rather than through their respective lines of business and functional areas)?

• Is there clarity as to roles and responsibilities regarding management of the priority enterprise risks:
  – Is there an enterprisewide view as to what they are?
  – Is there a risk owner assigned to manage each risk?
  – Are there gaps (no risk owner who makes decisions with respect to managing the risk and designing and monitoring risk management capabilities) to be filled?
  – Are there overlaps (too many risk owners, effectively diluting accountability) to be eliminated?
  – Are compensation practices incenting the desired behaviors?

• What is the quality of the communications and cooperation between the CRO and:
  – The business units?
  – The back-office risk management functions?
  – Key functional units (e.g., IT, legal, HR, etc.)?
  – Validation units (e.g., internal audit, compliance, etc.)?

• Are there unique market, credit, operational and other risks inherent in the organization’s lines of business requiring special attention? For example, are derivatives being used to speculate on markets or to hedge risk? If so:
  – Whose activities create the risks and why (e.g., if derivatives are used to hedge risks, what is being hedged, how is it being done and for how long)?
  – Do the organization’s systems provide sufficient disclosure regarding the risks?
  – Are the sources of the risks and how they affect operations known and understood?
  – Are valuations appropriate (e.g., are derivatives positions marked to market)?
  – Does the compensation structure sufficiently balance short-term versus long-term interests, or does it encourage unacceptable risk-taking?
  – Who is overseeing the management of the risks?
  – Do any of these risks require one or more risk units to house and maintain the competencies needed to assess and manage them enterprisewide?

Depending on the answers to these questions, an appropriate risk management oversight structure is designed with an emphasis on keeping it as simple as possible.
Conclusion

The CRO has an important role to play. The regulators’, CEO’s and board’s expectations for the function must be carefully considered and, given those expectations, the function must be positioned for success appropriately. We have discussed six key success factors in this paper. We have cited three studies providing an indication of the “current state” and evidencing progress since the financial crisis. We have offered suggestions to enhance further the CRO’s positioning and have recommended some steps CROs might take to identify enhancements in how their function is positioned within their respective organizations. Supported by effective board risk oversight, an effectively positioned CRO can assist the institution in gaining the “winning hand.”

---

About Protiviti

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our Financial Services Industry Team

We assist financial services companies in identifying, measuring and managing the myriad risks they face. With our commitment to service, people, resources and values, we are the service provider of choice for financial institutions of all types and sizes.

Our consultants are experienced professionals. Many have decades of experience working in the financial services industry. Located in offices across the globe, they include former industry executives, former regulators and a broad range of subject-matter experts who have firsthand knowledge of the issues on which they provide advice. Our internal commitment to training ensures that our consultants remain current on important industry issues. Armed with tested tools and methodologies, our consultants provide pragmatic, cost-effective and value-added solutions to your company.

At Protiviti, we understand the challenges faced by financial services companies. Our solutions are designed to help your company turn these challenges into competitive advantages.

Contact

Carol Beaumier  
Managing Director  
+1.212.603.8337  
carol.beaumier@protiviti.com

Cory Gunderson  
Managing Director  
+1.212.708.6313  
cory.gunderson@protiviti.com

Giacomo Galli  
Managing Director  
+39.02.6550.6303  
giacomo.galli@protiviti.it

Acknowledgements

We thank Cory Gunderson and Jim DeLoach for leading the project to develop this white paper.
<table>
<thead>
<tr>
<th><strong>THE AMERICAS</strong></th>
<th><strong>EUROPE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>United States</strong></td>
<td><strong>France</strong></td>
</tr>
<tr>
<td>Alexandria</td>
<td>Paris</td>
</tr>
<tr>
<td>Atlanta</td>
<td></td>
</tr>
<tr>
<td>Baltimore</td>
<td></td>
</tr>
<tr>
<td>Boston</td>
<td></td>
</tr>
<tr>
<td>Charlotte</td>
<td></td>
</tr>
<tr>
<td>Chicago</td>
<td></td>
</tr>
<tr>
<td>Cincinnati</td>
<td></td>
</tr>
<tr>
<td>Cleveland</td>
<td></td>
</tr>
<tr>
<td>Dallas</td>
<td></td>
</tr>
<tr>
<td>Denver</td>
<td></td>
</tr>
<tr>
<td>Fort Lauderdale</td>
<td></td>
</tr>
<tr>
<td>Houston</td>
<td></td>
</tr>
<tr>
<td>Kansas City</td>
<td></td>
</tr>
<tr>
<td>Los Angeles</td>
<td></td>
</tr>
<tr>
<td>Milwaukee</td>
<td></td>
</tr>
<tr>
<td>Minneapolis</td>
<td></td>
</tr>
<tr>
<td>New York</td>
<td></td>
</tr>
<tr>
<td>Orlando</td>
<td></td>
</tr>
<tr>
<td>Philadelphia</td>
<td></td>
</tr>
<tr>
<td>Phoenix</td>
<td></td>
</tr>
<tr>
<td>Pittsburgh</td>
<td></td>
</tr>
<tr>
<td>Portland</td>
<td></td>
</tr>
<tr>
<td>Richmond</td>
<td></td>
</tr>
<tr>
<td>Sacramento</td>
<td></td>
</tr>
<tr>
<td>Salt Lake City</td>
<td></td>
</tr>
<tr>
<td>San Francisco</td>
<td></td>
</tr>
<tr>
<td>San Jose</td>
<td></td>
</tr>
<tr>
<td>Seattle</td>
<td></td>
</tr>
<tr>
<td>Stamford</td>
<td></td>
</tr>
<tr>
<td>St. Louis</td>
<td></td>
</tr>
<tr>
<td>Tampa</td>
<td></td>
</tr>
<tr>
<td>Washington, D.C.</td>
<td></td>
</tr>
<tr>
<td>Woodbridge</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ASIA-PACIFIC</strong></th>
<th><strong>Italy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Australia</strong></td>
<td><strong>Bahrain</strong></td>
</tr>
<tr>
<td>Brisbane</td>
<td>Manama*</td>
</tr>
<tr>
<td>Canberra</td>
<td></td>
</tr>
<tr>
<td>Melbourne</td>
<td></td>
</tr>
<tr>
<td>Perth</td>
<td></td>
</tr>
<tr>
<td>Sydney</td>
<td></td>
</tr>
<tr>
<td><strong>China</strong></td>
<td><strong>Kuwait</strong></td>
</tr>
<tr>
<td>Beijing</td>
<td>Kuwait City*</td>
</tr>
<tr>
<td>Hong Kong</td>
<td></td>
</tr>
<tr>
<td>Shanghai</td>
<td></td>
</tr>
<tr>
<td>Shenzhen</td>
<td></td>
</tr>
<tr>
<td><strong>Indonesia</strong></td>
<td><strong>United Arab Emirates</strong></td>
</tr>
<tr>
<td>Jakarta**</td>
<td>Abu Dhabi*</td>
</tr>
<tr>
<td><strong>Japan</strong></td>
<td><strong>Oman</strong></td>
</tr>
<tr>
<td>Osaka</td>
<td>Muscat*</td>
</tr>
<tr>
<td>Tokyo</td>
<td></td>
</tr>
<tr>
<td><strong>Singapore</strong></td>
<td><strong>Peru</strong></td>
</tr>
<tr>
<td>Singapore</td>
<td>Lima*</td>
</tr>
</tbody>
</table>

* Protiviti Member Firm
** Protiviti Alliance Member

© 2013 Protiviti Inc. An Equal Opportunity Employer. PRO-PKIC-0113-080
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.